



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/727,479	12/04/2003	Mark Kraus	MS1-2715US	6237
22801	7590	01/31/2008	EXAMINER	
LEE & HAYES PLLC 421 W RIVERSIDE AVENUE SUITE 500 SPOKANE, WA 99201			HA, LEYNNA A	
			ART UNIT	PAPER NUMBER
			2135	
			MAIL DATE	DELIVERY MODE
			01/31/2008	PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

**Advisory Action  
Before the Filing of an Appeal Brief**

<b>Application No.</b> 10/727,479	<b>Applicant(s)</b> KRAUS ET AL.	
<b>Examiner</b> LEYNNA T. HA	<b>Art Unit</b> 2135	

**--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --**

THE REPLY FILED 24 December 2007 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1.  The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:

- a)  The period for reply expires 3 months from the mailing date of the final rejection.  
b)  The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**NOTICE OF APPEAL**

2.  The Notice of Appeal was filed on \_\_\_\_\_. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

**AMENDMENTS**

3.  The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because  
(a)  They raise new issues that would require further consideration and/or search (see NOTE below);  
(b)  They raise the issue of new matter (see NOTE below);  
(c)  They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or  
(d)  They present additional claims without canceling a corresponding number of finally rejected claims.

NOTE: \_\_\_\_\_. (See 37 CFR 1.116 and 41.33(a)).

4.  The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).  
5.  Applicant's reply has overcome the following rejection(s): \_\_\_\_\_.  
6.  Newly proposed or amended claim(s) \_\_\_\_\_ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).  
7.  For purposes of appeal, the proposed amendment(s): a)  will not be entered, or b)  will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.  
The status of the claim(s) is (or will be) as follows:  
Claim(s) allowed: \_\_\_\_\_.  
Claim(s) objected to: \_\_\_\_\_.  
Claim(s) rejected: 1-34.  
Claim(s) withdrawn from consideration: \_\_\_\_\_.

**AFFIDAVIT OR OTHER EVIDENCE**

8.  The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).  
9.  The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing of a good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).  
10.  The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

**REQUEST FOR RECONSIDERATION/OTHER**

11.  The request for reconsideration has been considered but does NOT place the application in condition for allowance because:  
See Continuation Sheet.  
12.  Note the attached Information Disclosure Statement(s). (PTO/SB/08) Paper No(s). \_\_\_\_\_  
13.  Other: \_\_\_\_\_.

Continuation of 11. does NOT place the application in condition for allowance because: claims 1-10 are not entered because they contain new limitations that was not presented prior to the Final rejection (9/19/2007).

Regarding the argument for claim 23 on pg.14 (1<sup>st</sup> paragraph) and pg.15 (3<sup>rd</sup> paragraph):

Applicant is unable to find Cromer disclosing a bootloader is stored in the protected storage. Cromer discloses flash memory is an electrically erasable programmable read only memory (EEPROM) module and includes BIOS that is used to interface between the I/O devices and operating system (col.3, lines 23-26). Thus, the claimed flash memory can be given as an EEPROM. Further, Cromer discloses the encryption/decryption engine may access a protected storage device 262 where the protected storage may be implemented utilizing an electrically erasable storage device such as an EEPROM (col.4, lines 38-39 and 46-50). Hence Cromer reads on the EEPROM or flash memory is protected and that the bootloader or BIOS is stored therein.

Regarding the argument on pg.14 (3<sup>rd</sup> paragraph) and pg.15 (4<sup>th</sup> paragraph):

Applicant states that Cromer does not disclose an operating system in an unprotected area of flash memory and notes the BIOS is not an operating system. Claim 23 recites an operating system(OS) image in the unprotected area of flash memory. Thus, the claimed limitation is not an operating system but an operating system image. Cromer discloses a determination of whether a device contains a image of the operating system (col.5, lines 27-28) where the boot record for the image is read in from the device (col.5, lines 33-35). The boot record is then signed and the BIOS hashes the boot record where the signature is decrypted and compares the decrypted hash (col.5, lines 27-28), Evidently, Cromer shows the boot record of the OS image read from the device is not secured nor protected because the boot record is not signed nor authenticated when the record is read. Thus, shows the boot record of the image is stored in an unprotected area of the memory.

Regarding the argument on pg.14 (4<sup>th</sup> paragraph):

Applicant finds the rejection improper and referring to pg.2-3 of the current Office Action to the limitation of claim 23 that starts at "wherein". Examiner is confused if applicant is referring to the Final Office Action (9/19/2007) because pgs.2-3 does not traverse the limitation of claim 23 that starts at "wherein". The end of pg.2 through pg.3 in Final Office Action (9/19/2007), traverses the argument of end of pg.16 regarding an image of the operating system.

Regarding the argument on pg.16:

that Cromer does not disclose the claimed examine an image update...embedded in the image update. The image update can broadly be interpreted as an image that have been transformed or modified which is now updated with different information. The image update includes a signed catalog file embedded broadly suggests the image is signed and hashed. In addition, the claimed "if the image update should be programmed into the unprotected area of flash memory" broadly suggests "should" is a decision that is not necessarily resulting in one specific result and where it is probable that the image update can be programmed to an unprotected or protected memory.

Cromer discloses a need for authentication/authorization during a boot procedure on a computer system particularly in a computer network environment where booting is authorized with the operating system through authentication by a server system of the digital signature (col.1, lines 35-45 and 58-61). Cromer also discloses determining whether a first selected device contains an image of an operating system and a determination of the image is bootable (col.5, lines 28-31). The image being bootable is considered authenticated if it is determined the signature and hash of the image compares to the list of authorized OS boot record (col.5, lines 50-57). Hence, the image update that includes a signature and hash not on the list of authorized OS boot record is inherently not authorized and therefore does not ensure authorized access to an OS image. Thus, should the image update not be programmed in the memory have been determined since the authenticated image is determined to be booting in a protected manner.

Regarding the argument for claim 11 on pg.20:

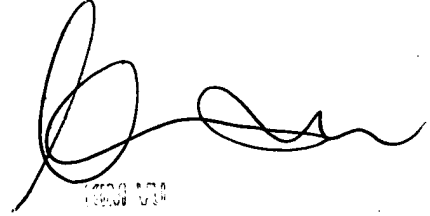
that Vanderpool does not discloses images of resource-sparing operating system images. Applicant has mention on pg.13, that resource-sparing operating system is well known in the art is often implemented in computing device that have limited storage and memory resources. Vanderpool suggests such resource-sparing operating system because his computer system have at least 16 Mbytes of RAM memory. This suggest a computing device having limited storage and memory resources (col.7, lines 15-18 and col.11, lines 31-35). Further, applicant indicated Vanderpool's images are in standard JPEG format. However, Vanderpool merely explains the compression/decompression process which performs decompression similar to a JPEG format (col.11, lines 36-41). Vanderpool does not insinuate the images are only in JPEG format. Vanderpool suggests creating a first hash of the created image (col.8, lines 4-15) and a second hash of the image from the catalog file where the second image obviously is a stored has that will be used as a reference to during the comparison process (col.8, lines 35-40). Innuendo, Cromer also suggests first and second hash. Thus, the Vanderpool and Cromer combination obviously teaches the claimed invention.

Regarding the argument for claim 11 on pg.21:

where Vanderpool fails to disclose blocking the use of the image to boot the computing device when the first hash and the second hash do not match is traversed. Cromer is combined with Vanderpool to teach this limitation. Cromer disclose a method and system for performing an authenticated boot of a computer system wherein the boot process for a computer system attached to a network is authenticated to ensure authorized access to an operating system image (col.1, lines 48-51 and col.5, lines 63-65). Cromer disclose a pre specified list of bootable devices is presented to the user for selection and a determination of the selected device whether it contains an image of a desired operating system (col.5, lines 22-35). Cromer discusses hashing the boot record with a hash algorithm and determines if the system boots approves or not whereby a password is requested if the boot records are not approved. Thereafter, if the password is invalid, then the system is halted (col.5, lines 40-47). Further, Cromer discloses comparing the decrypted received hash to a list of

authorized operating system boot record hashes (col.5, lines 55-56). Based on the whether the received hash matches an authorized hash, the system then boots or halts appropriately (col.5, lines 59-62). The list of authorized operating system boot record hashes is obviously the claimed second hash of the image from the catalog file because as established earlier, the catalog file is merely a listing of specific information. This reads on the claimed second hash of the image from the catalog file and blocking the use of the image to boot the computing device when the first hash and the second hash do not match. Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching of Vanderpool with the teach of blocking the use of the image to boot the computing device when the first hash and the second hash do not match as taught by Croimer because this ensures the boot process for a computer system is authenticated to ensure authorized access to an operating system image which avoids booting an incorrect operating system image (col.5, lines 55-67).

All dependent claims are also rejected by virtue of the dependency.



1000 000  
PATENT EXAM  
UNITED STATES PATENT AND TRADEMARK OFFICE